TunnellingSsh

rappel divers ssh:

X11

```
ssh -X monserveurclientX11
```

cf aussi la manip sur le authorizedkeys ...CopieFichiersHeliosServeurIremia

tunneling SSH

principe:

on est sur son poste (machine A). on veut acceder à une machine C. celle ci n'est pas accessible directement de la machine A. c'est le cas par exemple d'un serveur C en intranet, alors que la machine A est sur le reseau du provider.

solution

on va passer par une machine relay B. Voici la manip:

- on crée le tunnel:

```
ssh -v -L 1234:leffe:22 toto@fic-iremia
```

ou

```
ssh -v -L 1234:@C:22 compteSurB@B
```

leffe : machine C
fic-iremia : machine B (machine relais sur laquelle on dispose du compte toto)
on tape cette commande de la machine A.
un mot de passe est demandé, c'est le mo de passe de la machine B (fic-iremia dans notre cas).
on se retrouve avec une fenetre shell ouverte sur la machine B. on laisse comme ca, cette session ne sert qu'a créer le tunnel de A vers C (en passant par B).
22 -> le port ssh clasique
1234 -> le port d'entrée dans le tunnel.

- on se connecte de A vers B

de sa machine locale (A), on tape la commande suivante dans une autre fenetre:

```
ssh -v -p 1234 avelin@localhost
```

ou

```
ssh -v -p 1234 comptesurC@localhost
```

Ce faisant, on se connecte sur la machine C, avec un compte avelin. le mot de passe demande est celui de la machine C.

mise en pratique:

utilisez maloya (ou bastion.univ-reunion.fr bientot ...).
voici un exemple avec scp:

```
scp -v -P 1234 Documents/DEVIS/proforma_doc avelin@localhost:/tmp
```

en utilisant le tunnel précédemment créé, on copie de la machine locale un fichier `Documents/DEVIS/proforma_doc` vers la directory /tmp de la machine leffe, en se connectant par le compte avelin de la machine leffe.
attention, ici le P est en majuscule...

resolution probleme:

eventuellement, la connection dans le tunnel ssh ne fonctionne pas, message du type :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
c1:b7:c9:57:72:7b:ce:eb:ca:03:5a:06:04:f6:01:f1.
Please contact your system administrator.
```

enlever la ligne commencant par localhost dans le fichier `.ssh/known_hosts` sous votre directory de login.
ou utiliser le switch `-o "HostKeyAlias secure"` , par exemple :

```
ssh -p 1234  -o "HostKeyAlias secure"  avelin@localhost
```

tunnelling rsync

principe:

on utilise un tunnel ssh (cf premiere partie de la manip), pour rsync.
rsync, passera par ce tunnel pour faire la synchro d'un repertoire local avec un répertoire distant.

la commande classique rsync pour synchroniser 2 repertoires en passant par un tunnel ssh est

```
rsync -avz -e ssh  monRepASauver avelin@localhost:/chemin/distant
```

il faut maintenant creuser un tunnel et passer le flux rsync dans ce tunnel:

solution:

créer le tunnel :

```
ssh -N -v -L 1234:leffe:22 avelin@B
```

B est la machine bastion, *avelin* est le compte sur cette machine.
ensuite on fait le rsync en passant par ce tunnel:

```
rsync -avz -e "ssh -p1234"  Documents/DEVIS compteSurC@localhost:DEVIS_ESSAI
```

la directory locale Documents/DEVIS est synchronisée sur la machine distante derrière le firewall, dans la directory

DEVIS_ESSAI

Liens intéressants

- SSH tunnel manager
- Acces securise mail OSX
